

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-288522

(43)Date of publication of application : 31.10.1995

(51)Int.Cl. H04L 9/34  
H04K 1/06

(21)Application number : 06-306465

(71)Applicant : NEWS DATACOM LTD

(22)Date of filing : 09.12.1994

(72)Inventor : NACHMAN JACOB B  
TSURIA YOSSEF

(30)Priority

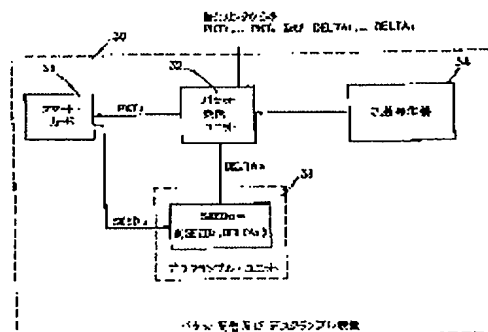
Priority number : 93 107967 Priority date : 09.12.1993 Priority country : IL

## (54) SYSTEM AND METHOD FOR PREVENTING HACKING

(57)Abstract:

PURPOSE: To prevent enciphered data from a transmitter from being deciphered by an unauthorized receiver in a network system.

CONSTITUTION: When a packet reception unit 32 receives packets PKT1-PKTn and offsets DELTA1-DELTA<sub>n</sub> from the transmitter and a random number from a random number generator 34 is '3', for example, the packet PKT3 is supplied to a smart card 36 and the offset DELTA3 is supplied to a descramble unit 38. The smart card calculates a seed SEED3 corresponding to the supplied packet and supplies it to the descramble unit. The descramble unit calculates a seed SEED0 based on the supplied SEED3 and offset DELTA3 and descrambles the received data while using the provided seed. Since descrambling is enabled only when the seed from the smart card is suitable, deciphering at the non-permitted receiver is prevented.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-288522

(43) 公開日 平成7年(1995)10月31日

(51) Int.Cl.<sup>9</sup>

H 0 4 L 9/34

H 0 4 K 1/06

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/ 00

B

審査請求 未請求 請求項の数32 O L (全 10 頁)

(21) 出願番号 特願平6-306465

(22) 出願日 平成6年(1994)12月9日

(31) 優先権主張番号 1 0 7 9 6 7

(32) 優先日 1993年12月9日

(33) 優先権主張国 イスラエル (I L)

(71) 出願人 594146065

ニューズ・データコム・リミテッド

NEWS DATACOM LTD

イギリス国ロンドン イー1・9エックス

ワイ, ヴァージニア・ストリート, ピー・

オー・ボックス 495

(72) 発明者 ジェイコブ・ベザレル・ナックマン

イスラエル国 ラマット・モディーム

73127, ハタマール・ストリート 3

(72) 発明者 ヨゼフ・ツーリア

イスラエル国 エルサレム 97276, シャ

ローム・シヴァン・ストリート 20

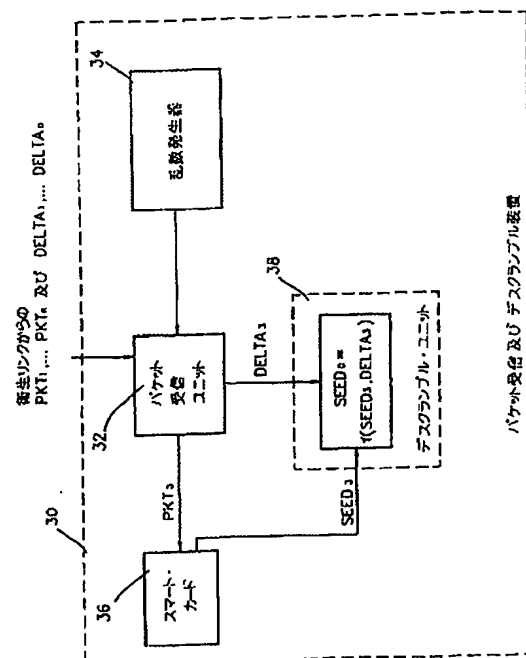
(74) 代理人 弁理士 湯浅 恭三 (外6名)

(54) 【発明の名称】 ハッキング防止システム及び方法

(57) 【要約】

【目的】 ネットワーク・システムにおいて、送信機からの暗号化されたデータが無許可受信機で非暗号化されないようにする。

【構成】 送信機からのデータ・パケット  $PKT_1 \sim PKT_n$  及びオフセット  $DELTA_1 \sim DELTA_n$  をパケット受信ユニット32が受信すると、乱数発生器34からの乱数が例えば“3”のとき、パケット  $PKT_3$  をスマート・カード36に供給し、かつオフセット  $DELTA_3$  をデスクランブル・ユニット38に供給する。スマート・カードは供給されたパケットに対応するシード  $SEED_3$  を計算してデスクランブル・ユニットに供給する。デスクランブル・ユニットは、供給されたシード  $SEED_3$  及びオフセット  $DELTA_3$  に基づいてシード  $SEED_0$  を計算し、該得られたシードを用いて受信されたデータをデスクランブルする。スマート・カードからのシードが適切な場合にのみデスクランブルが可能なので、無許可受信機での解読が防止される。



## 【特許請求の範囲】

【請求項1】 ネットワークにおけるハッキング防止システムであって、該ネットワークが、1つの送信機と、それぞれがシークレット・ナンバーによって独立にイネーブルされ、かつイネーブルされている場合には前記送信機から受信されたデータに応答して暗号化された情報を非暗号化する複数の受信機とを含んでいるハッキング防止システムにおいて、前記受信機のそれぞれは、前記データの少なくとも一部と、前記受信機の中の複数のものに関して異なっている関数手段とを用いて、異なる関数手段を有するそれぞれの受信機に関して異なっている第1のキーを発生する第1のキー発生器と、前記データの少なくとも一部と前記関数手段とを用いて、第2のキーを生じる第2のキー発生器と、前記第2のキーとともに前記第1のキーを利用して、前記複数の受信機のすべてにおいて同一である前記シークレット・ナンバーを生じるシークレット・ナンバー発生器とを備えており、ある受信機において傍受された第1及び第2のキーが、異なる関数手段を有する別の受信機をイネーブルすることができないようにしたことを特徴とするハッキング防止システム。

【請求項2】 請求項1記載のハッキング防止システムにおいて、前記受信機の少なくとも複数のものに関して異なっている前記関数手段は、乱数発生器によってその値が規定されることを特徴とするハッキング防止システム。

【請求項3】 請求項1記載のハッキング防止システムにおいて、前記第2のキー発生器は、単一のVLSIチップとして形成されていることを特徴とするハッキング防止システム。

【請求項4】 請求項3記載のハッキング防止システムにおいて、前記単一のVLSIチップは、スマート・カード上に配置されていることを特徴とするハッキング防止システム。

【請求項5】 請求項1記載のハッキング防止システムにおいて、前記第1のキー発生器、前記関数手段、及び前記シークレット・ナンバー発生器は、単一のVLSIチップとして構築されていることを特徴とするハッキング防止システム。

【請求項6】 請求項1記載のハッキング防止システムにおいて、前記第1のキー発生器、前記関数手段、前記シークレット・ナンバー発生器、及び前記第2のキー発生器は、単一のVLSIチップとして構築されていることを特徴とするハッキング防止システム。

【請求項7】 請求項6記載のハッキング防止システムにおいて、前記受信機のそれぞれは、前記VLSIチップの少なくとも1つを有していることを特徴とするハッキング防止システム。

【請求項8】 請求項1記載のハッキング防止システムにおいて、前記ネットワークはCATVネットワークで

あり、前記受信機はCATV受信及びデコーダとであることを特徴とするハッキング防止システム。

【請求項9】 1つの送信機と、それぞれがシークレット・ナンバーによって独立にイネーブルされ、かつイネーブルされている場合には前記送信機から受信されたデータに暗号化された情報を解読する複数の受信機と、を含むネットワークにおいて用いられるハッキング防止方法において、

前記データの少なくとも一部と前記受信機の中の少なくとも複数のものに関して異なる関数手段とを用いることによって、異なる関数手段を有するそれぞれの受信機に関して異なっている第1のキーを発生するステップと、前記データの少なくとも一部と前記関数手段とを用いることによって、第2のキーを生じるステップと、前記第2のキーと共に前記第1のキーを利用して、前記受信機のすべてに関して同一である前記シークレット・ナンバーを生じることによって、シークレット・ナンバーを発生するステップとを含んでおり、ある受信機において傍受された第1及び第2のキーが、異なる関数手段を有する別の受信機をイネーブルすることができないようにしたことを特徴とするハッキング防止方法。

【請求項10】 請求項9記載のハッキング防止方法において、前記受信機の少なくとも複数のものに関して異なっている前記関数手段は、乱数発生器であることを特徴とするハッキング防止方法。

【請求項11】 請求項9記載のハッキング防止方法において、前記第2のキーの発生は、単一のVLSIチップによって実行されることを特徴とするハッキング防止方法。

【請求項12】 請求項11記載のハッキング防止方法において、前記単一のVLSIチップは、スマート・カード上に配置されていることを特徴とするハッキング防止方法。

【請求項13】 請求項9記載のハッキング防止方法において、前記第1のキーの発生、前記関数手段の適用、及び前記シークレット・ナンバーの発生は、単一のVLSIチップによって実行されることを特徴とするハッキング防止方法。

【請求項14】 請求項9記載のハッキング防止方法において、前記キーの発生と、シークレット・ナンバーを生じる前記キーの組み合わせとは、単一のVLSIチップによって実行されることを特徴とするハッキング防止方法。

【請求項15】 請求項9記載のハッキング防止方法において、前記第1のキーの発生、前記関数手段の適用、及び前記シークレット・ナンバーの発生は、すべて、前記受信機のそれぞれにおいて実行されることを特徴とするハッキング防止方法。

【請求項16】 請求項9記載のハッキング防止方法において、該方法はCATVネットワークにおいて用いら

れ、前記キーの少なくとも一部と前記シークレット・ナンバーとの発生は、CATV受信機とデコーダとにおいて実行されることを特徴とするハッキング防止方法。

【請求項17】 加入者は、情報供給者、地理的位置、及び人口統計から成るパラメータの少なくとも1つによって個別に特徴付けられ、情報が、前記パラメータの少なくとも1つに従って各グループが前記情報の少なくとも一部分を受け取る権利を有している、それぞれのグループへと分類される複数の加入者に対して、情報源から送信され、1つの送信機と、それぞれが一人の加入者と関係しておりシークレット・ナンバーによって独立にイネーブルされ、イネーブルされている場合には前記送信機から受信されたデータに応答して暗号化された情報を解読する複数の受信機と、を含むネットワークにおいて用いられる、複数の加入者へ情報を選択的に送信する送信システムにおいて、前記受信機のそれぞれは、前記データの少なくとも一部と前記受信機の中の少なくとも複数のものに関して異なる関数手段とを用い、異なる関数を有するそれぞれの受信機に関して異なっている第1のキーを発生する第1のキー発生器と、前記データの少なくとも一部と前記関数手段とを用いて、第2のキーを生じる第2のキー発生器と、前記データの少なくとも一部を用いて、前記パラメータの少なくとも1つによって特徴付けられる第3のキーを生じる第3のキー発生器と、前記第1のキー、前記第2のキー、及び前記第3のキーを利用し、前記受信機のすべてに関して同一である前記シークレット・ナンバーを生じるシークレット・ナンバー発生器とを備えており、よって、ある受信機において傍受された第1及び第2のキーが、異なる関数手段を有する別の受信機をイネーブルすることができず、かつ、受信機のあるグループ内の受信機において傍受された第3のキーが、別のグループの受信機をイネーブルする事ができないようにしたことを特徴とする複数の加入者への情報の選択的送信システム。

【請求項18】 請求項17記載のシステムにおいて、前記受信機の少なくとも複数のものに関して異なっている前記関数手段は、乱数発生器であることを特徴とするシステム。

【請求項19】 請求項17記載のシステムにおいて、前記第2のキー発生器は、単一のVLSIチップによって形成されていることを特徴とするシステム。

【請求項20】 請求項19記載のシステムにおいて、前記単一のVLSIチップは、スマート・カード上に配置されていることを特徴とするシステム。

【請求項21】 請求項17記載のシステムにおいて、前記第1のキー発生器、前記関数手段、前記第3のキー発生器、及び前記シークレット・ナンバー発生器は、単一のVLSIチップによって形成されていることを特徴とするシステム。

【請求項22】 請求項17記載のシステムにおいて、前記第1のキー発生器、前記関数手段、前記第3のキー発生器、前記シークレット・ナンバー発生器、及び前記第2のキー発生器は、単一のVLSIチップによって形成されていることを特徴とするシステム。

【請求項23】 請求項22記載のシステムにおいて、前記受信機のそれぞれは、前記VLSIチップの少なくとも1つを有していることを特徴とするシステム。

【請求項24】 請求項17記載のシステムにおいて、前記ネットワークはCATVネットワークであり、前記受信機はCATV受信及びデコーダであることを特徴とするシステム。

【請求項25】 加入者が、情報供給者、地理的位置、及び人口統計から成るパラメータの少なくとも1つによって個別に特徴付けられ、情報が、前記パラメータの少なくとも1つに従って各グループが前記情報の少なくとも一部分を受け取る権利を有している個別のグループへと分類される複数の加入者に、情報源から送信され、1つの送信機と、それぞれが一人の加入者と関係しておりシークレット・ナンバーによって独立にイネーブルされ、イネーブルされている場合には前記送信機から受信されたデータに応答して暗号化された情報を解読する複数の受信機と、を含むネットワークにおいて用いられる、複数の加入者への情報の選択的送信方法において、前記データの少なくとも一部と前記受信機の中の少なくとも複数のものに関して異なっている関数手段とを用い、異なる関数手段を有するそれぞれの受信機に関して異なっている第1のキーを発生するステップと、前記データの少なくとも一部と前記関数手段とを用いて、第2のキーを生じるステップと、

前記データの少なくとも一部を用い、前記パラメータの少なくとも1つによって特徴付けられるキーである第3のキーを発生するステップと、前記第1のキー、前記第2のキー、及び前記第3のキーを利用し、前記受信機のすべてに関して同一である前記シークレット・ナンバーを生じることによって、シークレット・ナンバーを発生するステップとを含んでおり、ある受信機において傍受された第1及び第2のキーは、異なる関数手段を有する別の受信機をイネーブルすることができず、また、あるグループの受信機において傍受された第3のキーが、別のグループの受信機をイネーブルすることができないことを特徴とする送信方法。

【請求項26】 請求項25記載の方法において、前記受信機の少なくとも複数のものに関して異なっている前記関数手段は、乱数発生器であることを特徴とする方法。

【請求項27】 請求項25記載の方法において、前記第2のキーの発生は、単一のVLSIチップにおいて実行されることを特徴とする方法。

【請求項28】 請求項27記載の方法において、前記

単一のVLSIチップは、スマート・カード上に配置されていることを特徴とする方法。

【請求項29】 請求項25記載の方法において、前記第1のキーの発生、前記関数手段の適用、前記第3のキーの発生、及び前記シークレット・ナンバーの発生は、単一のVLSIチップにおいて実行されることを特徴とする方法。

【請求項30】 請求項25記載の方法において、前記キーの発生と、シークレット・ナンバーを生じるための前記キーの組み合わせとは、単一のVLSIチップにおいて実行されることを特徴とする方法。

【請求項31】 請求項25記載の方法において、前記第1のキー発生、前記関数手段の適用、前記キーの選択、及び前記シークレット・ナンバーの発生は、すべて、前記受信機のそれぞれにおいて実行されることを特徴とする方法。

【請求項32】 請求項25記載の方法において、該方法は、CATVネットワークにおいて用いられ、前記キーの少なくとも一部と前記シークレット・ナンバーとの前記発生は、CATV受信及びデコーダにおいて実行されることを特徴とする方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、一般には、秘密(secure)通信システムに関し、更に詳しくは、暗号化された情報を1つの場所から保護されていない場所にある複数の端末へ送信するための通信システムに関する。

【0002】

【発明の背景】 秘密通信システムにおける主な問題は、無許可の侵入(unauthorized penetration)である。この種の無許可侵入は、ハッキングと称される。ハッキングの問題を克服するために、いくつかの方法が用いられてきた。送信データの暗号化と通信者の認証とは、ハッキングをより困難にするのに用いられる方法である。克服が困難であると考えられているハッキングの方法の1つに、「マコーマック・ハッキング(McCormac Hack)」と呼ばれるものがある。この方法は、CATVシステムに理論的には応用可能であると信じられており、Frank Baylin等による“World Satellite TV and Scrambling Methods”(Baylin Publication 第2版、1991年、pp. 243~244)と、“Satellite Watch News”(1991年8月)に記載されている。この方法によれば、正当に許可されたデコーダからのデータ・ストリームがリアルタイムで抽出され、小型の無線周波数(RF)送信機を用いて空中で送信される。そして、このデータ・ストリームを用いて、複数の海賊(pirate)デコーダを付勢する。

【0003】

【発明の概要】 上記した従来例に鑑み、本発明は、正当に許可を得た端末からのデータ・ストリームを抽出して、該データ・ストリームを複数の海賊端末へ送信する可能性を、実質的に防止する方法及びシステムを提供することを目的とする。本発明においては、すべての形式における用語「端末(terminal)」は、通常の意味よりも広く用いられており、あらゆるタイプのコンピュータ端末、CATVデコーダ、遠隔のコンピュータ、及び遠隔のコンピュータ化されたステーションをカバーする。本発明においては、すべての形式における用語「シード(seed)」及び「キー(key)」は、通常の意味よりも広く交互に用いられており、データを暗号化/解読(すなわち、スクランブル/デスクランブル)するための暗号化/解読キーの少なくとも一部として用いられる、秘密あるいは秘密ではない、あらゆるタイプ又は他の記号(symbol)をカバーする。さらに本発明においては、用語「シークレット・ナンバー」が、本発明の目的のために、データの暗号化/解読(すなわち、スクランブル/デスクランブル)のために用いられる秘密のキーを表すために用いられる。

【0004】 本発明の好適実施例によれば、1つの送信機とそれぞれがシークレット・ナンバーによって独立にイネーブルされ(使用可能状態とされ)、イネーブルされている場合には前記送信機から受信されたデータに回答して暗号化された情報を解読する複数の受信機を含むネットワークにおいて用いられるハッキング防止システムであって、前記複数の受信機のそれぞれは、前記データの少なくとも一部と前記複数の受信機の中の少なくとも複数のものに対して異なる関数とを用い、異なる関数を有するそれぞれの受信機に対して異なっている第1のキーを発生する第1のキー発生器と、前記データと前記関数との少なくとも一部を用いて第2のキーを生じる第2のキー発生器と、前記第2のキーと共に前記第1のキーを利用し前記複数の受信機のすべてに対して同一である前記シークレット・ナンバーを生じるシークレット・ナンバー発生器とを備えており、これにより、第1の受信機において傍受された第1及び第2のキーにより、異なる関数を有する第2の受信機をイネーブルすることができないように構成された、ハッキング防止システムが提供される。

【0005】 本発明の別の好適実施例によれば、1つの送信機とそれぞれがシークレット・ナンバーによって独立にイネーブルされイネーブルされている場合には、前記送信機から受信されたデータに回答して、暗号化された情報を解読する複数の受信機を含むネットワークと共に用いられるハッキング防止方法であって、前記データの少なくとも一部と前記複数の受信機の中の少なくとも複数のものに対して異なる関数とを用いることによって、異なる関数を有するそれぞれの受信機に対して異なっている第1のキーを発生するステップと、前記データ

と前記関数との少なくとも一部を用いることによって、第2のキーを生じるステップと、前記第2のキーと共に前記第1のキーを利用し、前記複数の受信機のすべてに対して同一である前記シークレット・ナンバーを生じることによって、シークレット・ナンバーを発生するステップとを含んでおり、これにより、第1の受信機において傍受された第1及び第2のキーが、異なる関数を有する第2の受信機をイネーブルすることができないように構成されたハッキング防止方法が提供される。

【0006】更に別の本発明の好適実施例によれば、加入者が、情報供給者、地理的位置、及び人口統計から成るパラメータの少なくとも1つによって個別に特徴付けられ、前記パラメータの少なくとも1つに従って各グループが前記情報の少なくとも一部分を受け取る権利を有している異なるグループへと分類される複数の加入者に対して、情報が情報源から送信され、1つの送信機が、それぞれが一人の加入者と関連しかつシークレット・ナンバーによって独立にイネーブルされ、イネーブルされている場合には前記送信機から受信されたデータに暗号化された情報を解読する複数の受信機を含むネットワークにおいて用いられる、複数の加入者へ情報を選択的に送信する送信システムであって、前記複数の受信機のそれぞれは、前記データの少なくとも一部と前記複数の受信機の中の少なくとも複数のものに対して異なる関数とを用い、異なる関数を有するそれぞれの受信機に対して異なっている第1のキーを発生する第1のキー発生器と、前記データと前記関数との少なくとも一部を用いて、第2のキーを生じる第2のキー発生器と、前記データの少なくとも一部を用いて、前記パラメータの少なくとも1つによって特徴付けられる第3のキーを生じる第3のキー発生器と、前記第1のキー、前記第2のキー、及び前記第3のキーを利用し、前記複数の受信機のすべてに対して同一である前記シークレット・ナンバーを生じるシークレット・ナンバー発生器とを備えており、それにより、第1の受信機において傍受された第1及び第2のキーが、異なる関数を有する第2の受信機をイネーブルすることができないように構成され、かつ受信機の第1のグループの一部を形成する受信機において傍受された第3のキーが、受信機の前記グループの第2のものの一部を形成する受信機をイネーブルすることができないように構成され、複数の加入者への情報の選択的送信システムが提供される。

【0007】更にまた本発明の実施例によれば、加入者が、情報供給者、地理的位置、及び人口統計から成るパラメータの少なくとも1つによって個別に特徴付けられ、前記パラメータの少なくとも1つに従って各グループが前記情報の少なくとも一部分を受け取る権利を有している異なるグループへと分類される複数の加入者に、情報が情報源から送信され、1つの送信機が、それぞれが一人の加入者と関係しておりかつシークレット・ナン

バーによって独立にイネーブルされ、イネーブルされている場合には前記送信機から受信されたデータに暗号化された情報を解読する複数の受信機とを含むネットワークにおいて用いられる、複数の加入者へ情報を選択的に送信する送信方法であって、前記データの少なくとも一部と前記複数の受信機の中の少なくとも複数のものに対して異なる関数とを用い、異なる関数を有するそれぞれの受信機に対して異なっている第1のキーを発生するステップと、前記データと前記関数との少なくとも一部を用いて、第2のキーを生じるステップと、前記データの少なくとも一部を用い、前記パラメータの少なくとも1つによって特徴付けられるキーを生じることによって、第3のキーを発生するステップと、前記第1のキー、前記第2のキー、及び前記第3のキーを利用し、前記複数の受信機のすべてに対して同一である前記シークレット・ナンバーを生じることによってシークレット・ナンバーを発生するステップとを含んでおり、それにより、第1の受信機において傍受された第1及び第2のキーが、異なる関数を有する第2の受信機をイネーブルすることができないように構成され、また、受信機の第1のグループの一部を形成する受信機において傍受された第3のキーが、受信機の前記グループの第2のものの一部を形成する受信機をイネーブルすることができないように構成されている、複数の加入者への情報の選択的送信方法が提供される。

【0008】本発明の好適実施例によれば、前記複数の受信機の少なくとも複数のものに対して供給される異なる前記関数は、乱数発生器である。前記第2のキー発生器は、単一のVLSIチップに形成されることが好ましい。本発明の好適実施例によれば、前記VLSIチップは、スマート・カード上に配置されている。前記第1のキー発生器、前記関数、及び前記シークレット・ナンバー発生器は、単一のVLSIチップに形成されることが好ましい。本発明の好適実施例によれば、前記第1のキー発生器、前記関数、前記シークレット・ナンバー発生器、及び前記第2のキー発生器は、単一のVLSIチップに形成される。好ましくは、前記複数の受信機のそれぞれは、前記VLSIチップの少なくとも1つを含む。本発明の好適実施例によれば、前記ネットワークはCATVネットワークであり、前記複数の受信機はCATV受信機とデコーダとで構成される。

【0009】

【実施例】まず、図1を参照して、従来技術の「マコーマック・ハッキング」方法によって構成され動作する、理論的ハッキング・システムを説明する。通常は有効スマート・カード12によって動作される、許可を得た(authorized)デコーダ(許可デコーダ)10が、標準的なスマート・カード通信リンク15を介してマコーマック・ハッキング・インターフェース(MHI)ユニット14に結合されている。スマート・カード

12も、また、標準的なスマート・カード通信リンク16を介してMHIユニット14に結合されている。MHIユニット14は、スマート・カード12と許可デコーダ10との間で伝達される通信データの「匂いを嗅ぎ(s n i f f s)」,それを小型の無線送信機18に与える。無線送信機18は、データを、無線周波数(RF)リンク19を介して、仮想スマート・カード22に結合された無線受信機20に送信する。仮想スマート・カード22は、標準的なスマート・カード通信リンク25を介して、無許可デコーダ24に結合されている。このようにして、無許可デコーダ24は、許可デコーダ10を動作させるのと同じデータ・ストリームによって動作される。

【0010】別の例では、MHIユニット14は、許可デコーダ10の内部のユニットの間で通信されるデータの「匂いを嗅ぐ」。この例では、MHIユニット14は、通信リンク27を介して、マイクロプロセッサ28とデスクランブル・ユニット29との間の通信バス26にリンクされている。通信バス26は、デスクランブルのために必要なシークレット・ナンバーである「シード(SEED)」値を運ぶ。このようにして、シード値は抽出され、データのデスクランブルのために無許可デコーダに送信される。

【0011】次に、図2を参照して、本発明の好適実施例によって構成され動作する加入者側のバケット受信及びデスクランブル装置を説明する。本発明の好適実施例においては、一連の許可バケットPKT<sub>1</sub>~PKT<sub>n</sub>を含むデータ・ストリームが、情報源から、衛星リンクを介して、加入者のCATV受信機及びデコーダ(図示せず)の一部を形成するバケット受信及びデスクランブル装置30に送信される。一連のオフセット値DELTA<sub>1</sub>~DELTA<sub>n</sub>もまた、衛星リンクを介して、バケット受信及びデスクランブル装置30に送信される。好ましくは、各バケットは、オフセット値と対になっている。バケット受信及びデスクランブル装置30では、バケット受信ユニット(PRU)32が一連のバケットとオフセット値とを受信する。乱数発生器34が、乱数アルゴリズムを使用することによって、1からnの範囲の数をPRU32に与える。たとえば、3の数が乱数発生器34から発生されると、それに従って、対応するバケットすなわちPKT<sub>3</sub>がスマート・カード36に送信され、対応するオフセットすなわちDELTA<sub>3</sub>が、これは内部キーとして機能するのだが、デスクランブル・ユニット38に送信される。

【0012】スマート・カード36は、各バケットに対して適切なシード(SEED)を生じるアルゴリズムを使用する。スマート・カード36は、バケットPKT<sub>3</sub>を受信した場合には、対応するシードSEED<sub>3</sub>なるキーを生じ、これをデスクランブル・ユニット38に与える。PRU32、乱数発生器34、及びデスクランブル

・ユニット38はすべて、VLSIチップ等の1つの保護されたチップにおいて形成されることが好ましい。このようにして、乱数及びオフセットの通信は、変更されるすなわち「匂いを嗅がれる(s n i f f e d)」ことができなくなる。デスクランブル・ユニット38においては、PRU32とスマート・カード36とからそれぞれ受信されたキー、すなわちオフセット値DELTA<sub>3</sub>とシードSEED<sub>3</sub>は、次のような関数fによって用いられる。

【数1】  $f = f(\text{シード値}, \text{オフセット値})$

$SEED_0 = f(SEED_i, DELTA_i)$

ただし、SEED<sub>0</sub>はデータのデスクランブルに必要なシークレット・ナンバーであり、iは1~nの中の任意の整数で、乱数発生器34からの数である。したがって、i=3が選択された場合には、

【数2】  $SEED_0 = f(SEED_3, DELTA_3)$

である。

【0013】本発明の好適実施例においては、デスクランブル・ユニット38は、シードSEED<sub>0</sub>の値を発生する点でシークレット・ナンバー発生器として機能し、また、内部キーとスマート・カードからのキーとを受け取るキー受信機としても機能する。シードSEED<sub>0</sub>の値は、デスクランブル・ユニット38によって、データをデスクランブルするのに用いられる。デスクランブル・ユニット38がVLSIフォーマットを有している限りは、実際に不可能ではないにしても、シードSEED<sub>0</sub>の値を傍受(タップ)するのは困難であると考えられる。図2のハッキング防止システムは、スマート・カードを用いていないシステムと共にでも動作し得ることを理解されたい。その場合には、バケットPKT<sub>1</sub>~PKT<sub>n</sub>に対応するシード値は、スマート・カードにおいて用いられているのと類似のアルゴリズムを用いることによって、たとえば、PRU32、乱数発生器34、及びデスクランブル・ユニット38などの、バケット受信及びデスクランブル装置30の任意の適宜の1つの構成要素において作成される。乱数発生器34からの乱数が受信されると、対応する計算されたシード値と適切なオフセット値とが、デスクランブル・ユニット38に供給される。

【0014】次に、図3のフローチャートを参照して、図2の装置の動作を説明する。一連のデータ・バケットPKT<sub>1</sub>~PKT<sub>n</sub>と一連のオフセット値DELTA<sub>1</sub>~DELTA<sub>n</sub>とが、衛星リンクを介して受信されている。乱数発生アルゴリズムが、インデックス数1~nの中の1つを計算し選択するのに用いられる。乱数発生アルゴリズムの出力は、たとえば、インデックス3である。計算されたインデックス3に対応するバケット、すなわちPKT<sub>3</sub>が、スマート・カード36に送信される。スマート・カードにおいては、シードを計算するアルゴリズムを用いて、対応するシードSEED<sub>3</sub>を計算

するのに用いられる。そして、シードSEED<sub>3</sub>が、デスクランブル・ユニット38に供給される。計算されたインデックス数に対応するオフセット値、すなわちDELTA<sub>3</sub>は、デスクランブル・ユニット38に送信される。デスクランブル・ユニット38は、シークレット・ナンバー発生機能を有しているのでそれを用いることにより、シードSEED<sub>3</sub>とオフセット値DELTA<sub>3</sub>とを組み合わせ、衛星送信をデスクランブルするのに用いられるシークレット・ナンバーであるSEED<sub>0</sub>の値を計算する。このシード及びオフセット値は、シークレット・ナンバー発生のため以外にも用いられる。

【0015】次に、図4のフローチャートには、図2の装置の別の動作が示されている。該フローチャートは、シードの計算がスマート・カードにおいてではなく、図2のPRU32において実行されている点を除けば、図3のものと同様である。シードの計算はPRU32に限定されず、図2に示したバケット受信機及びデスクランブル・ユニット30を形成する保護されたVLSIチップの任意の部分において実行され得ることを理解された。

【0016】次に図5を参照するが、この図は、本発明の好適実施例による加入者ユニットの一部の一般化されたブロック図を示したものであり、異なる供給者によって供給された情報の受信機、又は、人口統計(demographics)や地理的な位置やそれ以外の任意のパラメータによってそれ以外の場合に相互に区別される受信機は、同じシークレット・ナンバーを用いてイネーブルされる。図5のシステムは、図2のシステムと比べて、さらに別のデータが、衛星リンクを介して情報源から受信され、バケット受信及びデスクランブル装置130において処理されている点を除いて、図2のものと同様である。図5のPRU132は、衛星リンクを介して、一連のバケットPKT<sub>1</sub>~PKT<sub>n</sub>と、上述のハッキング防止システムの一部で用いる一連の第1のオフセット値DELTA<sub>1</sub>~DELTA<sub>n</sub>と、一連の第2のオフセット値GAMMA<sub>1</sub>~GAMMA<sub>k</sub>とを受信する。

【0017】第2のオフセット値GAMMA<sub>1</sub>~GAMMA<sub>k</sub>は、プログラム供給者、地理的な位置、又は人口統計などの1つ又は複数の基準に基づいて、相互に区別され得る加入者受信機の別個のグループの間での区別に用いられる。このようにして、受信機の各グループは、第2のオフセット値の1つによって特徴付けられる。受信機のグループの特徴付けは、好ましくはバケット受信及びデスクランブル装置130における各デコーダの製造過程で入力される内部コード又は内部アルゴリズムか、又は、上述の例のようにデコーダとの最初の通信の際に1つの選択されたパラメータ又はパラメータ群に対してデコーダを有効化するスマート・カードにおけるアルゴリズムかのどちらかによって、達成され得る。したがって、このような特徴付けがなされると、各デコーダ

はイネーブルされ、それにより第2のオフセット値GAMMA<sub>1</sub>~GAMMA<sub>k</sub>の中から1つだけを選択する。これとは別に(又は、これに加えて)、デコーダの特徴付けは、第1のオフセット値だけを用いても達成することができる。その場合には、異なるデコーダが、ある特定のオフセット値だけを受信し、それ以外は受信しないように設定される。このようにして、第2のオフセット値の使用を必要としないようにすることもできる。

【0018】図5において、たとえば、デコーダがプログラム供給者を一意的に規定するオフセット値GAMMA<sub>2</sub>を選択するように特徴付けられると、PRU132は、該オフセット値GAMMA<sub>2</sub>をデスクランブル・ユニット138に供給する。たとえば、乱数3が乱数発生器134によって発生されると、PRU132は、対応するデータ・バケットPKT<sub>3</sub>をスマート・カード136に送信する。PRU132は、また、選択された乱数すなわちインデックス3に従って、一連のオフセット値DELTA<sub>1</sub>~DELTA<sub>n</sub>から1つのオフセット値、すなわちDELTA<sub>3</sub>を、デスクランブル・ユニット138に供給する。装置がユーザに提供された際に、各グループに対する加入者のためのスマート・カードは、別のグループの加入者に対してのスマート・カードとは異なっている。すなわち、グループ毎にスマート・カードが異なっており、それは、グループ毎のスマート・カードで異なるアルゴリズムを用いることによって、区別されている。したがって、たとえば、2人の異なる情報供給者によって動作される2つのデコーダで、同じ乱数、たとえば3が選択されたとしても、同じデータ・バケットすなわちPKT<sub>3</sub>が両方のスマート・カードに送信されるが、各スマート・カードは異なるシード値すなわちSEED<sub>3</sub>とSEED<sub>3</sub>\*とをそれぞれ計算により得ることになる。

【0019】そして上記した例においては、2つのデコーダのそれぞれが別個のプログラム供給者によって動作されるので、異なる第2のオフセット値GAMMA<sub>2</sub>とGAMMA<sub>3</sub>とがそれぞれデスクランブル・ユニット138に送信される。この2つのデコーダのデスクランブル・ユニット138においては、シークレット・ナンバー発生は、次のようにして実行される。

【数3】  $f = f(\text{シード値, 第1のオフセット値, 第2のオフセット値})$

$SEED_0 = f(SEED_3, DELTA_3, GAMMA_2)$

$SEED_0 = f(SEED_3*, DELTA_3, GAMMA_3)$

上述の方法によれば、同じSEED<sub>0</sub>を用いながら、1つの情報源から生じ加入者の別々のグループに向けられた情報をデスクランブルし、同時に、ある加入者群に向けられた認識可能な情報を別の加入者群には受信できなくすることができる。



【0020】図6のフローチャートは、図5の装置の動作が示している。一連のデータ・パケット $PKT_1 \sim PKT_n$ 、一連の第1のオフセット値 $DELTA_1 \sim DELTA_n$ 、及び一連の第2のオフセット値 $GAMMA_1 \sim GAMMA_k$ が、衛星リンクを介してパケット受信ユニット132で受信される。乱数発生アルゴリズムが、インデックス数 $1 \sim n$ の中から1つを計算し選択するのに用いられ、乱数発生器134の出力が、たとえば、インデックス3である場合、パケット $PKT_3$ がスマート・カード136に送信される。スマート・カードにおいては、シードを計算するアルゴリズムが用いられて、対応するシード $SEED_3^*$ を計算する。そして、得られたシード $SEED_3^*$ が、デスクランブル・ユニット138に供給される。計算されたインデックス数3に対応する第1のオフセット値 $DELTA_3$ は、パケット受信ユニット132からデスクランブル・ユニット138に供給される。供給者又は地域(jurisdiction)を識別する第2のオフセット値、たとえば $GAMMA_2$ もまた、デスクランブル・ユニット138に供給される。

【0021】デスクランブル・ユニット138では、 $SEED_3^*$ 、 $DELTA_3$ 、及び $GAMMA_2$ が、シークレット・ナンバー発生アルゴリズムを用いることによ

って組み合わせられ、衛星通信情報をデスクランブルするのに用いられるシークレット・ナンバーとなるシード $SEED_0$ の値が計算される。当業者は、本発明が以上で述べた内容に限定されないことを、理解されよう。むしろ、本発明の範囲は、冒頭の特許請求の範囲によってのみ定義される。

【図面の簡単な説明】

【図1】従来技術である「マコーマック・ハッキング」法に基づく理論的なハッキング・システムの一般化されたブロック図である。

【図2】本発明の好適実施例によって構成され動作する加入者ユニットの一部の装置のブロック図である。

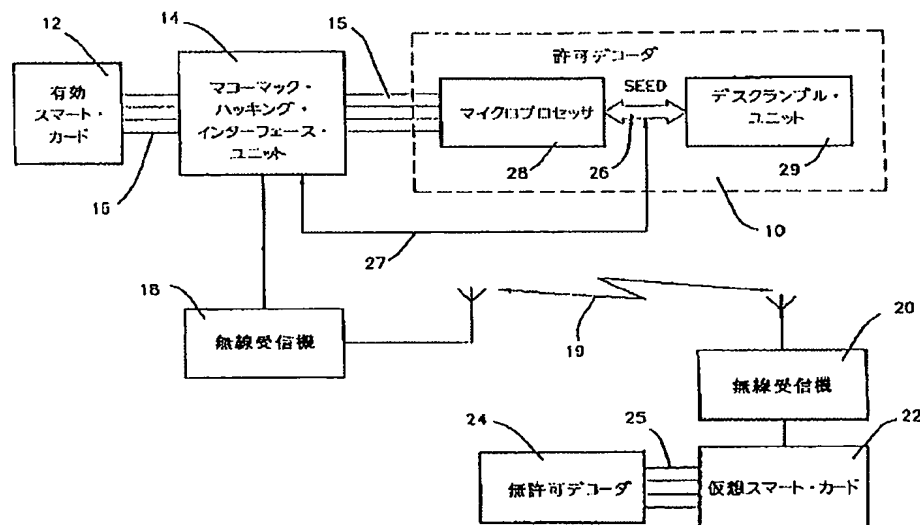
【図3】図2の装置の動作を説明するためのフローチャートである。

【図4】条件付きアクセス・カードを用いない場合の図2の装置の動作を説明するためのフローチャートである。

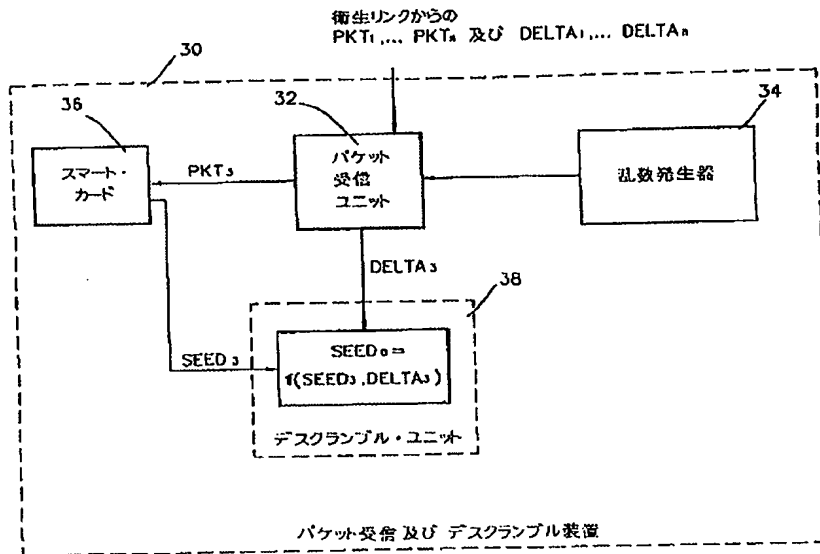
【図5】異なるパラメータによって特徴付けられる受信機を、同じシークレット・ナンバーを用いてイネールすることができる、本発明の好適実施例による加入者ユニットの一部の装置のブロック図である。

【図6】図5の装置の動作を説明するためのフローチャートである。

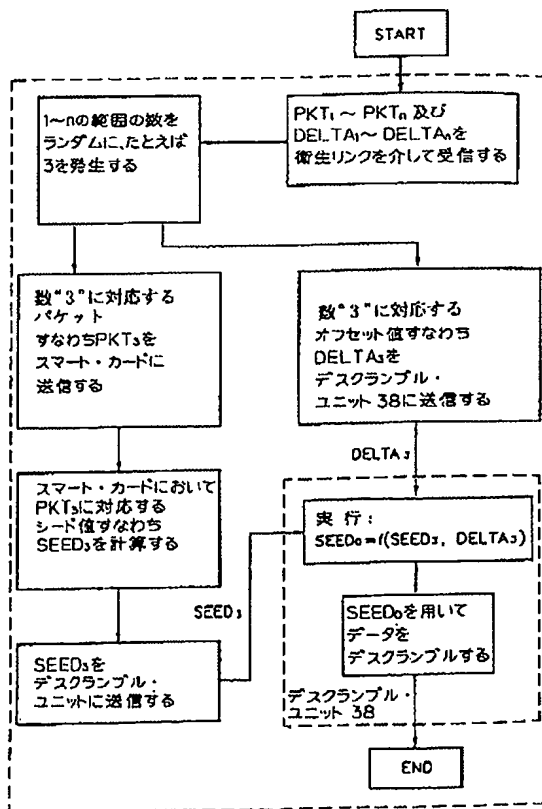
【図1】



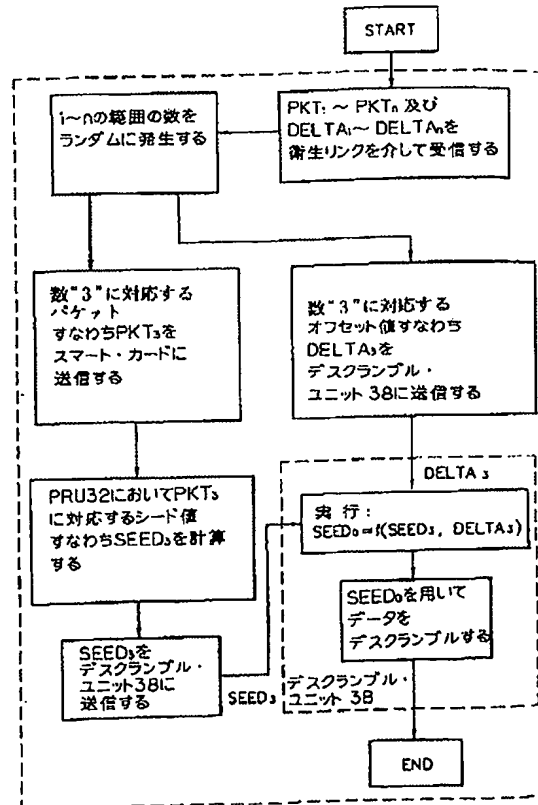
【図2】



【図3】

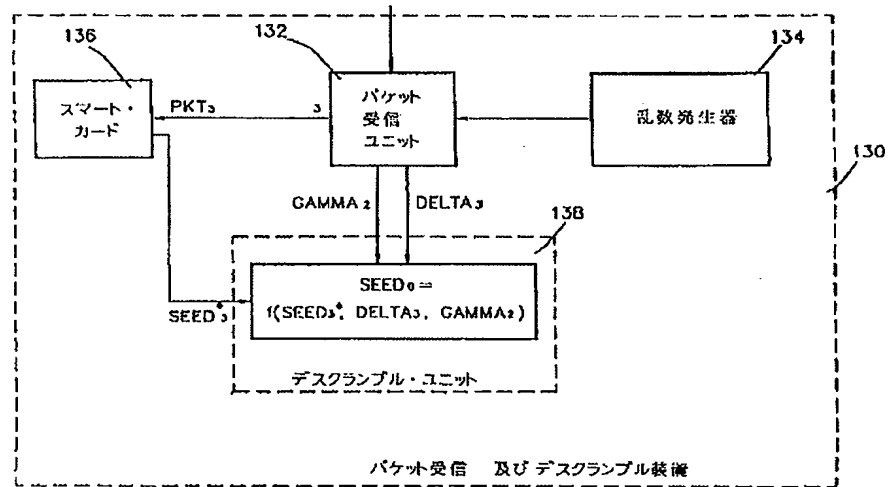


【図4】



【図5】

衛生リンクからの  
 $PKT_1, \dots, PKT_n, \Delta_1, \dots, \Delta_n$  及び  $\Gamma_1, \dots, \Gamma_k$



【図6】

